

Norton AntiVirus™ for Lotus Notes® Installation Guide

SYMANTEC.TM

NORTON

AntiVirusTM

FOR LOTUS NOTES®

Norton AntiVirus™ for Lotus Notes® Installation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 2.0

Copyright Notice

Copyright © 1997–1999 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make change without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, Peter Norton Group, 10201 Torre Avenue, Cupertino, CA 95014.

Trademarks

Symantec, Norton AntiVirus, Symantec AntiVirus for Macintosh, and Norton Utilities are trademarks of Symantec Corporation.

Windows is a registered trademark of Microsoft Corporation. Lotus and Lotus Notes are registered trademarks of Lotus Corporation. Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

NOTICE: SYMANTEC LICENSES THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE OPENING THIS PACKAGE, AS OPENING THE PACKAGE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN SYMANTEC IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN SIXTY DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

LICENSE AND WARRANTY:

The software which accompanies this license (the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. Except as may be modified by a license addendum which accompanies this license, your rights and obligations with respect to the use of this Software are as follows:

- You may:

- (i) use one copy of the Software on a single computer;
- (ii) make one copy of the Software for archival purposes, or copy the software onto the hard disk of your computer and retain the original for archival purposes;
- (iii) use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network;
- (iv) after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this agreement; and
- (v) if a single person uses the computer on which the Software is installed at least 80% of the time, then after returning the completed product registration card which accompanies the Software, that person may also use the Software on a single home computer.

- You may not:

- (i) copy the documentation which accompanies the Software;
- (ii) sublicense, rent or lease any portion of the Software;
- (iii) reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software; or
- (iv) use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version as a replacement of the prior version, unless you donate a previous version of an upgraded version to a charity of your choice, and such charity agrees in writing that it will be the sole end user of the product, and that it will abide by the terms of this agreement. Unless you so donate a previous version of an upgraded version, upon upgrading the Software, all copies of the prior version must be destroyed.

- Sixty Day Money Back Guarantee:

If you are the original licensee of this copy of the Software and are dissatisfied with it for any reason, you may return the complete product, together with your receipt, to Symantec or an authorized dealer, postage prepaid, for a full refund at any time during the sixty day period following the delivery to you of the Software.

- Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

- Disclaimer of Damages:

REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

- U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. §252.227-7014(a)(5) and 48 C.F.R. §252.227-7014(a)(1), and used in 48 C.F.R. §12.212 and 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. §12.212, 48 C.F.R. §252.227-7015, 48 C.F.R. §227.7202 through 227.7202-4, 48 C.F.R. §52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 10201 Torre Avenue, Cupertino, CA 95014.

- General:

This Agreement will be governed by the laws of the State of California. This Agreement may only be modified by a license addendum which accompanies this license or by a written document which has been signed by both you and Symantec. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: Symantec Customer Sales and Service, 10201 Torre Avenue, Cupertino, CA 95014.

SYMANTEC SOFTWARE LICENSE ADDENDUM

Notwithstanding any of the terms and conditions contained in the Symantec Software License, you may make and use up to that number of copies of the Software that is indicated on the License Authorization Coupon contained in your box. The coupon will constitute proof of your right to make and use such additional copies.

C O N T E N T S

Norton AntiVirus for Lotus Notes

About Norton AntiVirus	9
What is a computer virus?	10
How Norton AntiVirus works	10
Installing Norton AntiVirus for Lotus Notes	11
Minimum system requirements	11
Installation	12
Replicating the NAV Settings and NAV Log databases	13
Replicating the NAV Definitions database	15
Starting Norton AntiVirus for Lotus Notes	16
Using the Notes console window	17
Configuring scanning	18
Scheduling scans	20
Setting Global Options	21
Using the NAV Log	25
Managing the Quarantine	26
Maintaining current protection	31
About LiveUpdate	31
How to update virus protection	32
Updating virus protection without LiveUpdate	33

Symantec Service and Support Solutions

CD Replacement Form

Index

Norton AntiVirus for Lotus Notes

Norton AntiVirus secures your Lotus Notes environment against virus attack by protecting databases on Lotus Notes servers and monitoring email that is routed through the servers. Norton AntiVirus operation is transparent to users, with minimal performance degradation to the network.

Remember, however, the Lotus Notes environment is only one avenue a virus can use to penetrate your site. For a complete virus protection solution, make sure the appropriate workstation or server version of Norton AntiVirus is installed on every computer at your site as well.

About Norton AntiVirus

Norton AntiVirus (NAV) is completely integrated into the Lotus Notes environment. All scanning is configured and initiated from the NAV Settings database. All reports and virus dispositions are handled through the NAV Log database. Information about the product and how to use it is provided in the NAV Help database.

Norton AntiVirus for Lotus Notes can be configured to do any of the following:

- Eliminate viruses automatically on detection.
- Quarantine infected documents and email for administrator review.
- Delete infected items.

When viruses are detected, email notifications are sent, optionally, to specified administrators, document or email authors, and intended email recipients.

What is a computer virus?

A computer virus is a program designed in such a way that, when run, it attaches a copy of itself to another computer program or document. Thereafter, whenever the infected program is run or document is opened, the attached virus program is activated and attaches itself to yet other programs and documents.

In addition to replicating, viruses are generally programmed to deliver a payload. Most viruses simply display a message on a particular trigger date. Some, however, are programmed specifically to damage data by corrupting programs, deleting files, or reformatting disks.

Two classes of viruses compose the greatest threat in the Lotus Notes environment:

- Macro viruses, which infect word processing and spreadsheet documents (such as Microsoft Word or Excel)
- Program viruses, which infect executable files

The viruses spread as attachments or embedded OLE objects to documents written to Notes databases on servers and Notes email. Norton AntiVirus for Lotus Notes detects and eliminates these viruses.

How Norton AntiVirus works

Symantec engineers track reported outbreaks of computer viruses to identify new viruses. Once a virus is identified, information about the virus (a virus signature) is stored in a virus definitions file, which contains the necessary information to detect and eliminate the virus. When Norton AntiVirus scans for viruses, it is searching for these telltale virus signatures.

To supplement detection of known viruses, Norton AntiVirus includes a powerful new component called Bloodhound. With this advanced heuristic technology, Norton AntiVirus can detect a high percentage of new or unknown viruses not yet analyzed by anti-virus researchers.

The Norton AntiVirus LiveUpdate feature makes sure your virus protection remains current. Updated virus definitions files are provided by Symantec regularly. With LiveUpdate, Norton AntiVirus connects automatically to a special Symantec site, determines if your files need updating, downloads the proper files, and installs them in the proper location.

Installing Norton AntiVirus for Lotus Notes

The Norton AntiVirus setup program reads the Windows NT registry to locate the Lotus Notes server and default data directories. In addition to Norton AntiVirus registry keys, the following directories are located or created, as necessary:

- **\Notes**

Norton AntiVirus engine

- **\Notes\Data\NAV**

- **\Lotus\Domino\NAV (for R5)**

Norton AntiVirus databases (NAV.NSF, NAVLOG.NSF, and NAVHELP.NSF)

If updated virus definitions are going to be replicated to other Notes servers running Norton AntiVirus, NAVDEFS.NSF is created here after installation. See [“Replicating the NAV Definitions database”](#) on page 15 for more information.

- **\Program Files\Common Files\Symantec Shared**

Virus definitions files (used for all Norton AntiVirus products)

- **\Program Files\Symantec\LiveUpdate**

Technology to download virus definitions files and program updates (used for all Symantec products)

Minimum system requirements

Administrator-level privileges to both Windows NT and the Lotus Notes server are required to install Norton AntiVirus for Lotus Notes.

Operating system	Windows NT Server 3.51 with Service Pack 5 or Windows NT Server 4.0 with Service Pack 3
Lotus Notes	Notes Server version 4.5 or higher (version 4.52 or higher is required to repair infected OLE objects embedded in documents)
Processor	90 MHz Pentium or higher
Memory	64 MB (performance is dependent on server load)
Disk space to install	20 MB

Available disk space for processing	50 MB minimum (the location for temporary files is a Global Option that can be changed after installation)
--	--

Installation

Norton AntiVirus for Lotus Notes version 2.0 can be installed over existing Norton AntiVirus installations (either version 1.0 or 2.0). A setup option lets you retain existing NAV settings or scheduled scans.

To install Norton AntiVirus for Lotus Notes:

- 1 Shut down the Lotus Notes server.
- 2 Shut down your Lotus Notes client.
- 3 Run \NAVNOTES\SETUP.EXE from the Norton AntiVirus CD.

Note: If you have multiple Lotus Notes partitions on the same server, separate Norton AntiVirus databases are required for each partition. Setup detects and lets you specify on which partitions to install Norton AntiVirus.

- 4 After the Norton AntiVirus installation completes, restart the Lotus Notes server.

When the Lotus Notes server is restarted, the Norton AntiVirus databases are created from templates and placed in the NAV subdirectory of your default Data directory. A README.TXT file and a NAVREPL.TXT file are placed in this directory as well.

- 5 Start your Lotus Notes client.
- 6 Select the workspace tab on which you want to place Norton AntiVirus.

Some administrators prefer to label and dedicate a single tab to Norton AntiVirus.
- 7 From the File menu, choose Database, then Open.
- 8 In the NAV directory, double-click the NAV Settings database (NAV.NSF) to place its icon on the tab.

To facilitate enterprise-wide management of Norton AntiVirus, the NAV databases can be replicated to other servers running Norton AntiVirus for Lotus Notes. With replication, Norton AntiVirus settings can be configured from a single server, virus incidents and statistics can be reported for all

servers, and only a single virus definitions update is required to maintain current protection for all servers.

Replicating the NAV Settings and NAV Log databases

The NAV Settings database, NAV.NSF, can be replicated to other Notes servers running Norton AntiVirus for Lotus Notes 2.0. The NAV server task, ntask, monitors NAV.NSF for changes to the NAV settings through replication and reloads the settings on the local server. NAV settings can be distributed by manual or scheduled replication.

The following subset of settings in the NAV Settings database are replicated between Notes servers:

- Auto-Protect settings
- Global options settings
- All scheduled scans

See “[Configuring scanning](#)” on page 18 for information about NAV settings.

The NAV Log database, NAVLOG.NSF, stores server messages, reports of virus incidents, and scan summaries. It also provides access to quarantined documents and documents Norton AntiVirus backs up before eliminating viruses. Through replication, you can maintain a master NAV Log that automatically includes virus incidents and statistics reports from other Notes servers running Norton AntiVirus. See “[Using the NAV Log](#)” on page 25 for information about the NAV Log.

Before Norton AntiVirus is installed

To prepare for NAV Settings and NAV Log replication:

- 1 Select a server in your organization to be the master Norton AntiVirus server.
- 2 Install Norton AntiVirus for Lotus Notes 2.0 on the server and start the Notes server on that machine.
- 3 Before installing Norton AntiVirus on other servers, create replicas of the newly installed NAV.NSF and NAVLOG.NSF databases in the <Notes server data directory>\NAV directory on the other Notes servers.

Note: The Lotus Notes server default data directory is <drive>:\NOTES\DATA\NAV. For R5, the Lotus Notes server default data directory is <drive>:\LOTUS\DOMINO\NAV.

- 4 Install Norton AntiVirus for Lotus Notes 2.0 on the other servers, but keep the already replicated NAV.NSF and NAVLOG.NSF databases. This is an option of the Norton AntiVirus setup program.
- 5 Ensure that you and LocalDomainServers are in the Access Control List of NAV.NSF and NAVLOG.NSF, with Manager access and Delete Documents enabled. The LocalDomainServers group should contain all of the servers to which you plan to replicate.

Any changes made to NAV settings on any of the Notes servers are distributed to the other replicas when a manual or scheduled replication occurs. After replication, the new NAV settings are reloaded automatically.

Note: Replication save conflicts can be avoided by permitting only the Notes administrator in charge of anti-virus policy to edit the NAV settings on each of the Notes servers.

For the log, initiate push replication from the NAV Log replicas to the master NAVLOG.NSF. In this way, logging of virus incidents across the network is centralized.

After Norton AntiVirus is installed

If Norton AntiVirus for Lotus Notes (either version 1.0 or 2.0) is already installed on a Notes server to which the NAV Settings or NAV Log databases are being replicated, you must stop the NAV server task on that server before replicating the database.

To stop the NAV server task on a “replica” Notes server:

- 1 Type **TELL NAV QUIT** in the server console window.
- 2 Replicate the NAV Settings and NAV Log databases from the master Notes server to the replica Notes servers.

If prompted to overwrite an existing NAV.NSF or NAVLOG.NSF, respond Yes. This overwrites the existing databases with the new replicas.

- 3 Type **LOAD NTASK** to restart NAV.

Replicating the NAV Definitions database

The NAV Definitions database, NAVDEFS.NSF, stores updated virus definitions. The database can be replicated to other Notes servers running Norton AntiVirus for Lotus Notes 2.0 so that only a single LiveUpdate is required to maintain current protection on all servers. See “[Maintaining current protection](#)” on page 31 for information.

The Notes server on which the master NAVDEFS.NSF is created should be the machine that downloads new virus definitions updates through a scheduled LiveUpdate.

Note: Use of the NAV Definitions database is only required if you plan to replicate updated virus definitions. If you do not intend to replicate virus definitions, you do not need to create the NAV Definitions database.

To prepare NAV Definitions for replication:

- 1 Select a Notes server in your organization that will be used to download updated virus definitions.
- 2 After installing Norton AntiVirus on the server, click LiveUpdate in the Norton AntiVirus main window.
- 3 In the LiveUpdate form, click Create NAV Definitions Database.
- 4 Enable and schedule the LiveUpdate.
- 5 Make sure that Save Downloaded Virus Definitions In The NAV Definitions Database is checked.
- 6 Ensure that you and LocalDomainServers are in the Access Control List of NAVDEFS.NSF, with Manager access and Delete Documents enabled. The LocalDomainServers group should contain all of the servers to which you plan to replicate.
- 7 Create replicas of the master NAVDEFS.NSF database on the other Notes servers running Norton AntiVirus.

The definitions database must reside in the <Notes server data directory>\NAV directory on the other Notes servers and be called NAVDEFS.NSF.

The next time a scheduled LiveUpdate runs, any updated virus definitions are downloaded and a new NAVDEFS.NSF document is created. The new virus definitions set is marked as active. The updated definitions are distributed to the other replicas when a manual or scheduled replication occurs. The NAV server task checks for a new virus definition set at 10 minute intervals.

Starting Norton AntiVirus for Lotus Notes

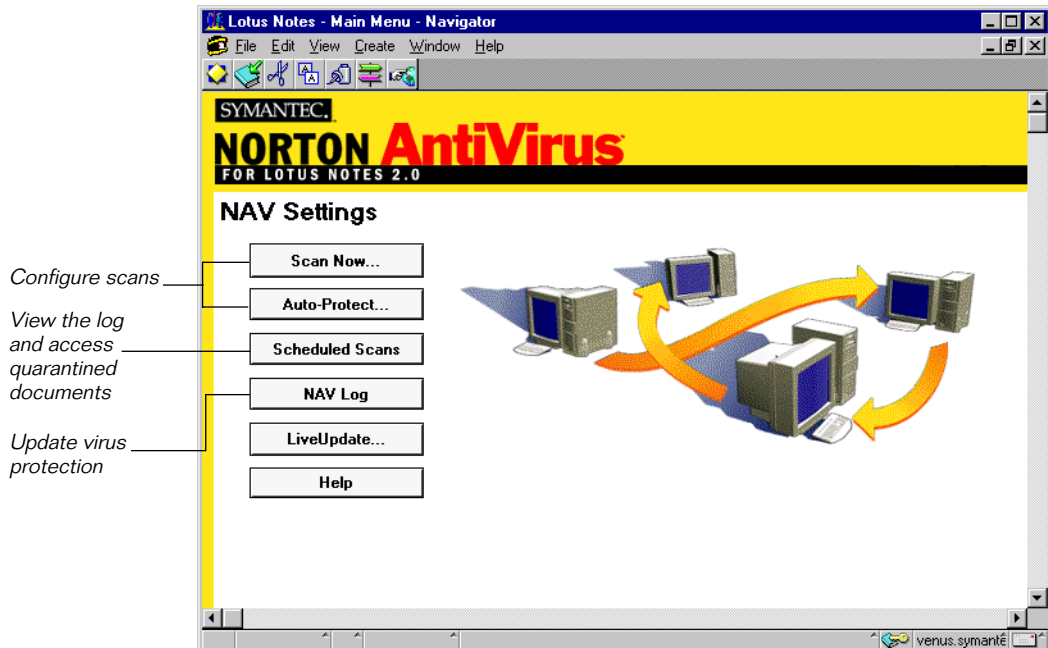
Norton AntiVirus runs as a Notes server task. Every time the server is started, Norton AntiVirus protection begins as well. Management and configuration tasks are accessed through the Lotus Notes client.

To access Norton AntiVirus for Lotus Notes:

- Double-click the NAV Settings icon on your Lotus Notes workspace tab.

The first time you click the NAV Log and Help buttons, icons for these databases are placed on your Lotus Notes workspace tab as well.

Norton AntiVirus main window



To get help while using Norton AntiVirus, do any of the following:

- In the Norton AntiVirus main window, click the Help button to display the help table of contents.
- In the Action bar of any form or view, click the Help button to access the context-specific help topic.

- In any form, click the group label that precedes options for a brief pop-up description of the options.

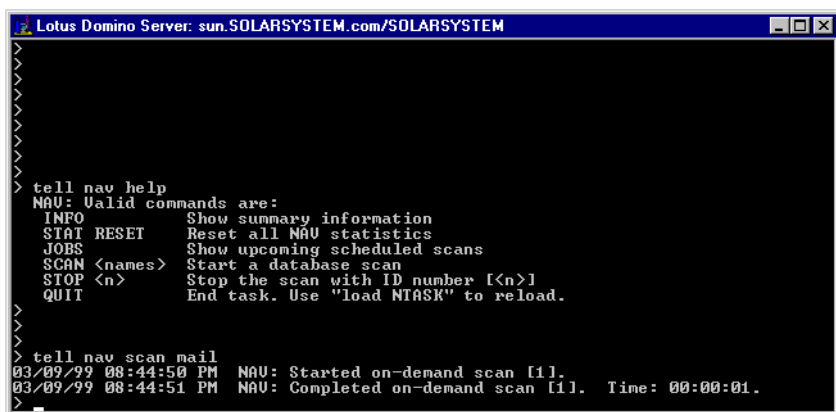
Using the Notes console window

You can view and manage some Norton AntiVirus operations directly from the Notes server console window. Use the following syntax at the command prompt:

TELL NAV <command>

Command	Description
HELP	Lists Norton AntiVirus console commands.
INFO	Summary of Norton AntiVirus operation.
STAT RESET	Clears processing details.
JOBS	Lists upcoming scheduled scans. The job names are the ones entered when the scan was scheduled.
SCAN <names>	Initiates a scan of the specified databases. A number is displayed in the console window to identify each scan.
STOP <n>	Stops the scan with the specified number.
QUIT	Stops the Norton AntiVirus server process. To reload Norton AntiVirus, enter LOAD NTASK at the console command prompt.

Lotus Notes server console window



```

Lotus Domino Server: sun.SOLARSYSTEM.com/SOLARSYSTEM
>
>
>
>
> tell nav help
NAU: Valid commands are:
  INFO      Show summary information
  STAT RESET Reset all NAU statistics
  JOBS      Show upcoming scheduled scans
  SCAN <names> Start a database scan
  STOP <n>   Stop the scan with ID number [<n>]
  QUIT      End task. Use "load NTASK" to reload.
>
> tell nav scan mail
03/09/99 08:44:50 PM NAU: Started on-demand scan [1].
03/09/99 08:44:51 PM NAU: Completed on-demand scan [1]. Time: 00:00:01.
>

```

Configuring scanning

Norton AntiVirus scans can be initiated at any time, scheduled to run at specific times, or set to monitor database writes and email routing in real time.

To configure and initiate scans:

- 1 Double-click the NAV Settings icon on your Lotus Notes workspace tab to open the Norton AntiVirus main window.
- 2 In the Norton AntiVirus main window, click one of the following buttons to configure scanning:
 - Scan Now
An on-demand scan you can invoke at any time. You can select either all databases in your default Data directory or select specific databases or directories to scan. The scan does not begin until you click Start The Scan in the form. You can also restrict the scan to documents that have been modified since a specified date.
 - Auto-Protect
Real-time scanning of database writes on the server and email as it is routed through the server. Auto-Protect is your best insurance to detect and eliminate viruses before they have a chance to spread.
 - Scheduled Scan
Scans that run automatically and without administrator intervention. Use scheduled scans to ensure that your databases remain virus-free. You can also restrict the scan only to documents that have been modified after the next scheduled scan start time.

Each scan type uses a three-section form to configure the scan:

Basics	What and when to scan.
Scan Options	Which global options to apply and what to do if a virus is detected. Click the Global Options button in the Action bar of any form to modify settings.
Notifications	Whom to notify when a virus is detected. Click the Global Options button in the Action bar of any form to identify administrators and customize the body of the email notification.

As an example, the following figure shows the form to configure Auto-Protect real-time scanning. Click the option group labels for pop-up help about the options or click Help in the Action bar for detailed context help.

Auto-Protect scan form

Click for procedural help

Click the group labels for pop-up help with options

Auto-Protect

Basics

When to scan

- ☒ Email routing
- ☒ Document writes

Ignore the following server processes

If ncompact, nfixup, nupdall, nupdate (nntask is always excluded)

[Reset to defaults](#)

Databases

- ☒ Exclude specified databases and directories from scans (see Global Options)

Attachments

- ☐ Scan all attachments regardless of extension
- ☒ Scan attachments with specified file extensions (see Global Options)

When a virus is detected

- ☐ Notify only
- ☐ Delete the infected attachment
- ☐ Quarantine the document
- ☒ Repair the infected attachment

If unable to repair

- ☐ Notify only
- ☐ Delete the infected attachment
- ☒ Quarantine the document

Virus detection notifications

Send email alerts to the following (see Global Options)

- ☒ Specified users (administrators and others)
- ☒ Document author
- ☒ Intended recipients

Scheduling scans

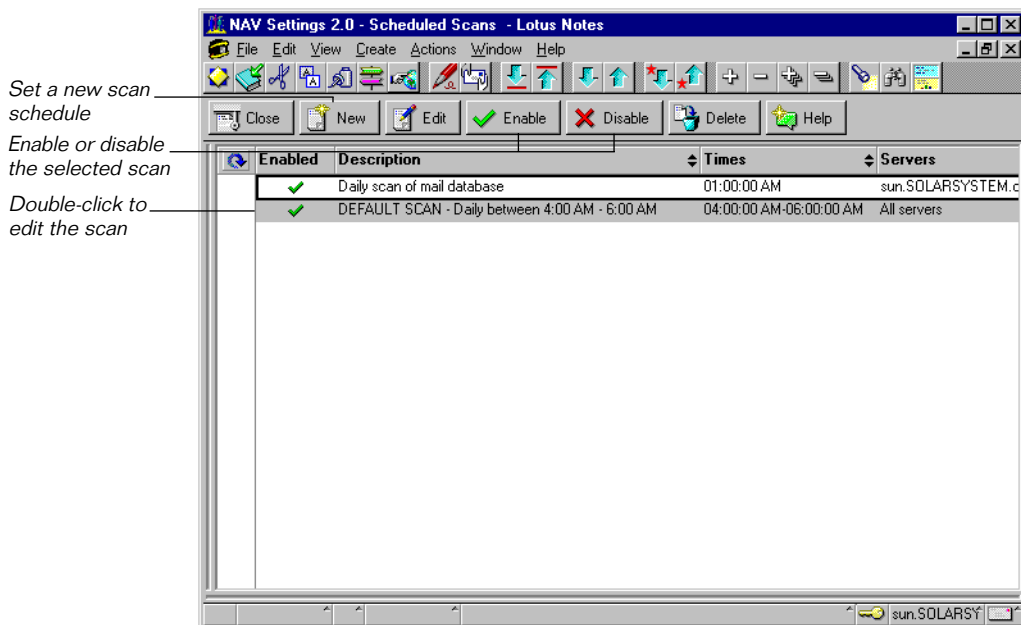
Scans can be scheduled to repeat at the same time on specified days or repeat at a specified interval on specified days.

To schedule scans:

- 1 In the Norton AntiVirus Main window, click Scheduled Scans.
- 2 Do one of the following:
 - Double-click an existing scan to modify it.
By default, a scan of all databases in the Data directory of the server is configured to run daily between 4:00 A.M. and 6:00 A.M.
 - Click New to configure and schedule a scan.

Note: For domains with multiple servers, there is an option when configuring the scan to schedule the same scan to run on one or more servers. The scan itself can be scheduled from any server in the domain. For server-specific changes to scheduled scans, the NAV.NSF database must be replicated to the appropriate servers.

Scheduled Scans



Setting Global Options

Global options can be accessed and configured from any of the scan forms. These options apply to all scans. Changes made, for example, from the Scan Now form, apply to Auto-Protect and all already-scheduled scans. Once set, however, you probably do not need to change them.

Global Options form

Global Options

Scan options

Specified file extensions

[Reset to defaults](#)

Databases and directories to exclude from scans

Backup options

Back up documents before repairing attachments

☒ Yes ☐ No

Back up documents before deleting attachments

☒ Yes ☐ No

Processing options

Bloodhound™ virus detection technology

☐ Off ☐ Low ☒ Med ☐ High

Repair signed documents (will break signatures on repaired documents)

☒ Yes ☐ No

Directory for temporary files (leave blank for Windows default)

Logging options

What to display

☒ General messages

☐ General messages and viruses that couldn't be eliminated

☐ General messages and all virus events

Where to save (in addition to console window and Notes event log)

☒ NAV Log

☒ Windows NT Event Log

Virus detection notification options

Specified users (administrators and users)

Custom text to administrators

Subject:

Body:

☒ Report action taken by Norton AntiVirus

☒ Include virus information from the log

To set global options:

- 1 In the Norton AntiVirus main window, click Scan Now, Auto-Protect, or Scheduled Scan.
- 2 At the top of the scan form, click Global Options.
- 3 Set the options, which are summarized in the following tables.
- 4 Click Save, then Close.

Scan options

Specified file extensions	When configuring a scan (Scan Now, Auto-Protect, or Scheduled Scan) and Scan Attachments With Specified Extensions is selected, Norton AntiVirus only scans attachments whose file extensions are listed. This setting reduces resource demand and speeds processing during the scan. The default list includes file types commonly at risk of infection. If your environment includes executable files with non-standard extensions, add them to the list. In most cases, the default list is appropriate.
Databases and directories to exclude from scans	When configuring a scan (Scan Now, Auto-Protect, or Scheduled Scan) and Exclude Specified Databases And Directories From Scans is checked, Norton AntiVirus always skips the listed databases and directories. For example, you may have documentation or reference databases that are not at risk of virus infection because they cannot be modified by users.

Backup options

Back up documents before repairing	As a data safety precaution, Norton AntiVirus can store a backup copy of an infected document before making the repair to eliminate the virus. In the NAV Log, click Backup Documents to view the list and delete or restore backups.
Back up documents before deleting	As a data safety precaution, Norton AntiVirus can store a backup copy of an infected document before deleting an infected attachment. In the NAV Log, click Backup Documents to view the list and delete or restore backups.

Processing options

Bloodhound virus detection technology	Bloodhound is an advanced heuristic technology that detects a high percentage of any new or unknown viruses that have not yet been analyzed by anti-virus researchers. Because there is a small processing overhead, you can set the level of resource demand. In most cases, the Med (medium) setting is appropriate.
Repair signed documents	To eliminate viruses from signed documents, Norton AntiVirus must break the signature. If Repair Signed Documents is disabled and a virus is detected, a signed document is treated as one that cannot be repaired.
Directory for temporary files	<p>Norton AntiVirus uses the default Windows TEMP directory for processing during scans. You should have at least 50 MB of free space on this drive. If necessary, you can specify a directory on another drive with more space available.</p> <p>If you use another anti-virus product, disable scanning of this directory to prevent interference with Norton AntiVirus operation. Other Norton AntiVirus products are aware of this location and do not require further configuration.</p>

Logging options

What to display	Determines what information is reported during Norton AntiVirus processing.
Where to save	Norton AntiVirus system information is always reported in the Notes server console window and stored in the Miscellaneous Events view of the Notes log. In addition, you can save this information in the Server Messages view of the NAV Log and the Windows NT Event Log.

Virus detection notifications

**Administrators
(and specified
users)**

Select administrators and other users who should be notified when a virus is detected. Use the email alert to advise them to attend to users whose workstations are infected.

**Document
authors**

Use the email alert to instruct users how to eliminate the virus source, such as scanning with a workstation version of Norton AntiVirus.

**Document
recipients**

If your policy is to quarantine infected documents, let users know whom to contact to release the document. If your policy is to delete infected attachments, advise them to contact the document author to resend an uninfected version.

Using the NAV Log

The NAV Log stores server messages, reports of virus incidents, and scan summaries. It also provides access to quarantined documents and documents Norton AntiVirus backs up before eliminating viruses.

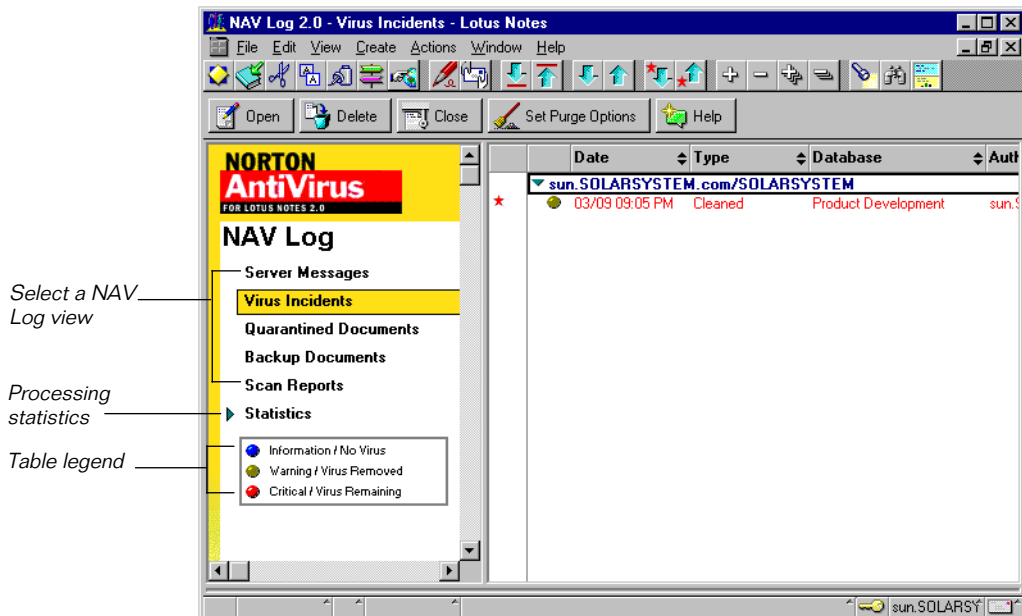
To prevent the log from growing too large, a purge agent runs every night at 1:00 A.M. By default, Virus Incidents are purged after 365 days. Other NAV Log entries are purged after 30 days. To change the number of days that log entries are stored, open the NAV Log and click Set Purge Options on the Action Bar.

Note: Your current user account must have administrator-level privileges for agents on the server where NAV Log resides to enable the purge agent.

To access the NAV Log:

- 1 Do one of the following:
 - Click the NAV Log icon on your Notes workspace tab.
 - In the Norton AntiVirus main window, click NAV Log.

NAV Log (Server Messages)

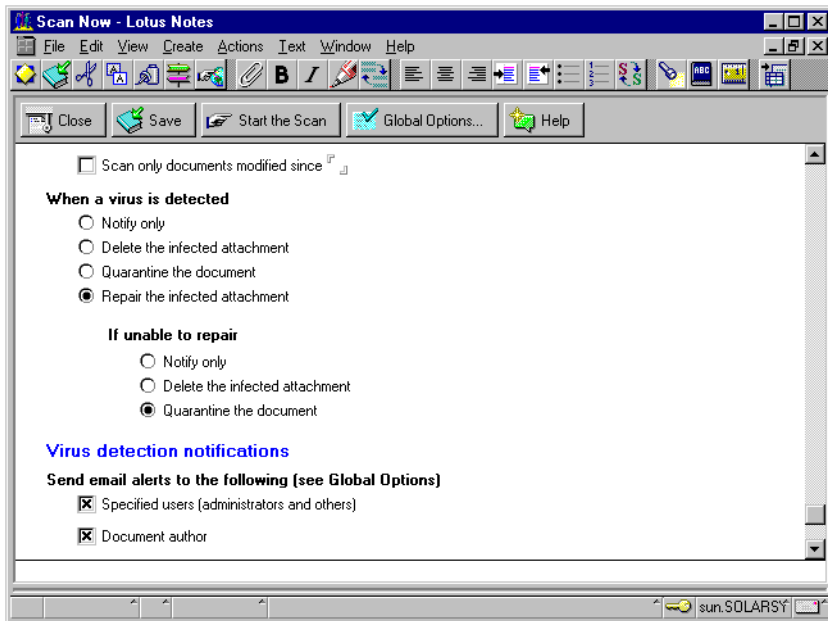


- 2 Click to select one of the following log views:
 - Server Messages
All server-related events.
 - Virus Incidents
All virus detections.
 - Quarantined Documents
Infected documents that have not been repaired.
 - Backup Documents
As a data safety precaution, Norton AntiVirus can be configured (from Global Options) to store a backup copy of documents that contain infected attachments before attempting a repair.
 - Scan Reports
Summaries of scheduled and on-demand scans.
 - Statistics
Statistics for Norton AntiVirus processing.

Managing the Quarantine

When using the Scan Now, Auto-Protect, or Scheduled Scan forms to configure scans, indicate in the Scan Options section what to do if a virus is detected. The following figure shows this section of the form.

Scan Now, Auto-Protect, and Scheduled Scan forms



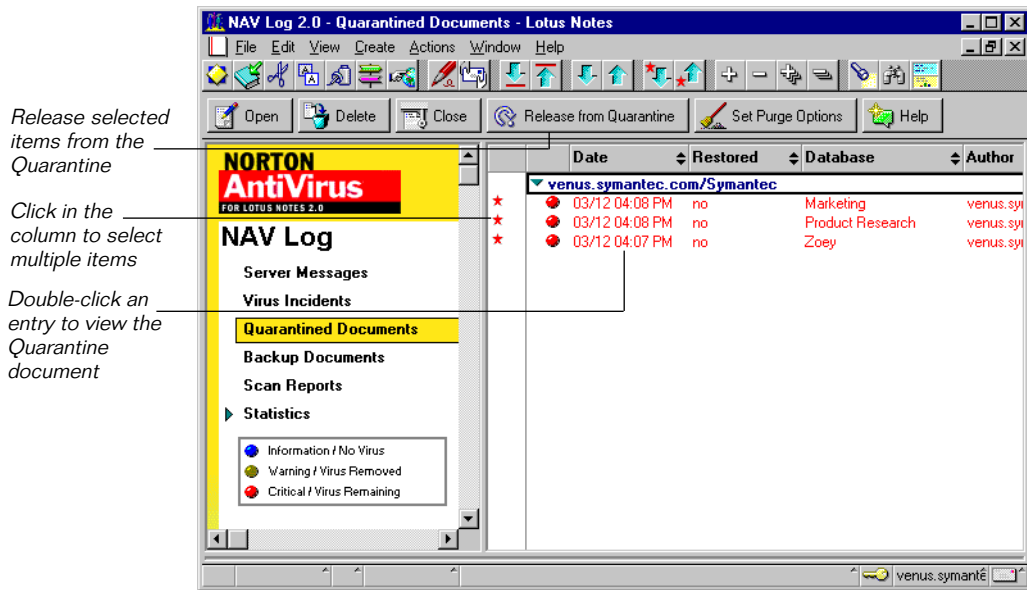
Documents are quarantined for one of two reasons:

- Your scan configuration is set to quarantine documents if a virus is detected.
- Your scan configuration is set to repair infected attachments, but quarantine any documents that have attachments that cannot be repaired.

To manage items in the Quarantine:

- 1 Open the NAV Log and click Quarantine Documents.

NAV Log (Quarantined Documents)



- 2 Select an item in the list.
- 3 Do one of the following:
 - Click Release.

Depending on the item, the database write is completed or the email is delivered. See the next procedure for information on how to handle infected attachments.

Make sure the document or email no longer contains infected attachments. If you release a document that still has infected attachments, it will only be quarantined again.
 - Click Delete.

The infected document or email is deleted and the entry is removed from the Quarantine.

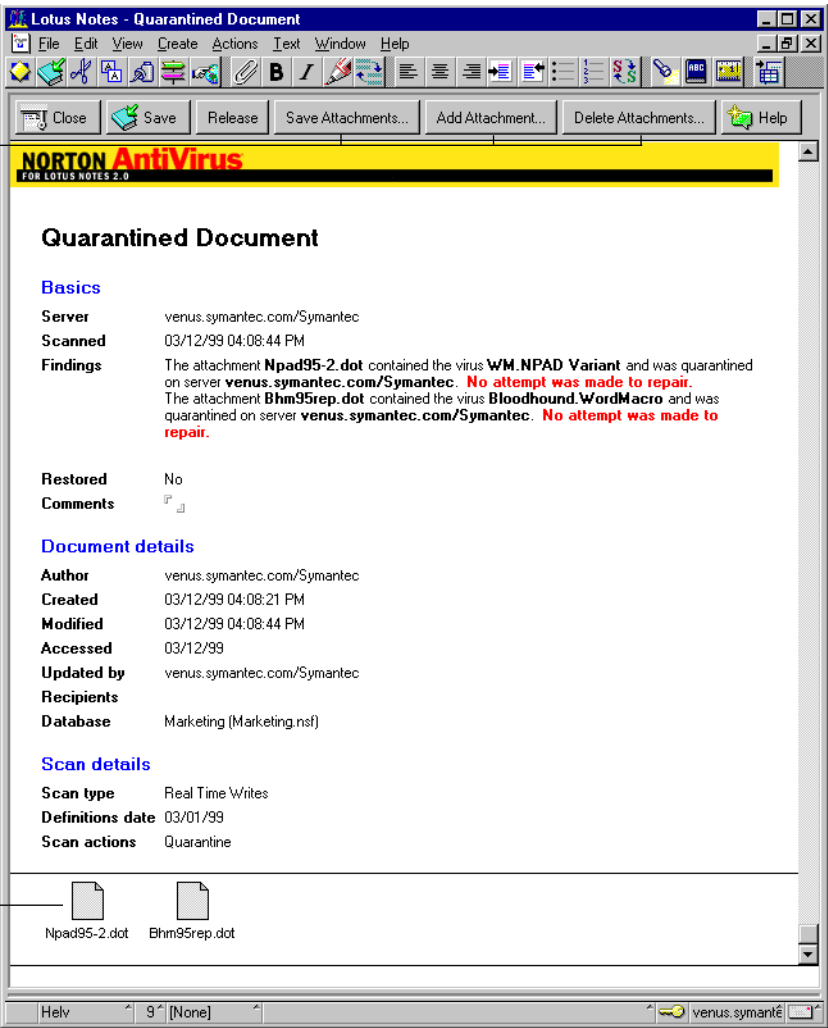
To manage infected attachments:

- 1 Open the NAV Log and click Quarantine Documents.
- 2 Double-click an item in the Quarantine to view the Quarantine Item document.

- 3 Click one of the following:
 - Save Attachments
Saves the infected attachment as a file.
 - Add Attachments
Before releasing the document from the Quarantine, you can add a newly repaired compressed file, replace an infected file with a known good copy, or, perhaps, add a procedural file with instructions to scan a workstation.
 - Delete Attachments
Removes the infected attachments. You are prompted before the deletion takes place.
- 4 Click Release to release the document or email.

Quarantine Item document

Actions for infected attachments



Attachments

Maintaining current protection

Norton AntiVirus relies on up-to-date information to detect and eliminate viruses. One of the most common reasons you may have a virus problem is that you have not updated your protection files since you installed the product. Symantec regularly supplies updated virus definitions files, which contain the necessary information about all newly discovered viruses.

About LiveUpdate

With LiveUpdate, Norton AntiVirus connects automatically to special Symantec sites and determines if your virus definitions need updating. If so, it downloads the proper files and installs them in the proper location.

LiveUpdate also checks for and downloads program patches to Norton AntiVirus for Lotus Notes, if available. An email is sent to administrators specified in Global Options with the name and location of the patch. Program modifications are never made outside of your control.

LiveUpdate connects to Symantec sites in one of two ways:

- Internet
Symantec maintains an Internet site for LiveUpdate use.
- Bulletin Board System (BBS)

LiveUpdate can also connect to a LiveUpdate BBS. To minimize your telephone toll charges, Symantec maintains several LiveUpdate BBSS around the world. LiveUpdate reads your location information and dials the closest BBS automatically.

Generally, you do not have to do anything to configure LiveUpdate. The only requirement is an Internet connection or a modem. When LiveUpdate runs, it determines how to connect automatically. If you want, you can force LiveUpdate to connect with a specific method. For example, you may have more than one modem, more than one Internet connection, or a modem and an Internet connection, and want LiveUpdate to connect using a particular one.

To configure LiveUpdate operation:

- 1 Open the Windows NT control panel.
- 2 Double-click LiveUpdate.

- 3 Modify your settings in the LiveUpdate Properties.
The LiveUpdate online help explains all options.

How to update virus protection

To immediately update virus definitions:

- 1 In the Norton AntiVirus main window, click LiveUpdate.
- 2 Click the Run LiveUpdate Now button.

To schedule automatic LiveUpdates:

- 1 In the Norton AntiVirus main window, click LiveUpdate.

LiveUpdate form

Check to enable
the scheduled
LiveUpdate

The screenshot shows the 'LiveUpdate - Lotus Notes' window. The title bar includes 'File', 'Edit', 'View', 'Create', 'Actions', 'Text', 'Window', and 'Help'. Below the title bar is a toolbar with icons for Close, Save, Help, Run LiveUpdate Now, and Create NAV Definitions Database. The main content area has a yellow header with 'NORTON AntiVirus FOR LOTUS NOTES 2.0'. Below this, the 'LiveUpdate' section is titled. Under 'Basics', it states: 'LiveUpdate downloads the latest virus definition files and product patches from Symantec. New virus definition files are automatically put to use after the download. Product patches must be applied manually. Use the LiveUpdate Control Panel to configure your connection method.' Under the 'Schedule' section, there are three options: 'Enable LiveUpdate' (checked), 'Save downloaded virus definitions in the NAV Definitions database' (unchecked), and 'Time of day to run:' (set to 04:00 AM). Below this, 'Days to run:' are set to 'Daily' (selected), 'Weekly', and 'Monthly'.

- 2 In the Schedule section of the form, check Enable LiveUpdate.
Uncheck to disable LiveUpdate.

- 3 If you plan to replicate the virus definitions database to other Notes servers, check Save Downloaded Virus Definitions In The NAV Definitions Database.

Don't check this option if you have NAV installed on a single Notes server or do not plan to replicate the definitions database. See ["Replicating the NAV Definitions database" on page 15](#) for more information.

- 4 Enter the time of day that LiveUpdate runs and select the frequency.
Specify an off-peak time in a high-traffic network.
- 5 At the top of the form, click Save, then Close.

Updating virus protection without LiveUpdate

Symantec provides the latest virus definitions files with a program called Intelligent Updater, available for download from our website (<http://www.symantec.com>) and other sources listed in the Service and Support Solutions in this guide. If you don't have a modem or Internet connection available, you can get the updates by mail.

To update virus definitions files:

- 1 Download (or copy) Intelligent Updater to any directory on the server.
- 2 Run Intelligent Updater.
Intelligent Updater reads the Windows NT registry and installs the necessary files in the proper locations.
- 3 Delete Intelligent Updater (for example, 0204I32A.EXE).

Symantec Service and Support Solutions

Symantec is committed to excellent service worldwide. Our goal is to provide you with professional assistance in the use of our software and services, wherever you are located.

Technical Support and Customer Service solutions vary by country. If you have questions about the services described below, please refer to the section “Worldwide Service and Support” at the end of this chapter.

Registering your Symantec product

To register your Symantec product, please complete the registration card included with your package and drop the card in the mail. You can also register via modem during the installation process (if your software offers this feature) or via fax to (800) 800-1438 or (541) 984-8020.

LiveUpdate Subscription Policy

Retail customers: With the purchase of this product, you receive 12 free months of unlimited online use of LiveUpdate. Renewal subscriptions are available for \$3.95 per year.

After using this product for ten months, you will be prompted to subscribe when you begin a LiveUpdate session. Simply follow the onscreen instructions. After your one-year free subscription ends, you must renew your subscription before you can complete a LiveUpdate session.

To order, do one of the following:

- In the United States, call Customer Service at (800) 441-7234
- Outside the United States, contact your local Symantec office or representative
- Visit our website at: www.shop.symantec.com

Corporate Customers: Contact your Symantec representative for information about LiveUpdate subscription pricing.

Virus definitions update disk

If you don't have a modem to obtain virus definitions files using the Internet, CompuServe, America Online, or the Symantec BBS, you can order regular updates from Symantec to arrive by mail. This service requires a fee.

To order, do one of the following:

- In the United States, call (800) 441-7234.
- Outside the United States, contact your local Symantec office or representative.

Technical support

Symantec offers an array of technical support options designed for your individual needs to help you get the most out of your software investment.

World Wide Web

The Symantec World Wide Web site (<http://service.symantec.com>) is the doorway to a set of online technical support solutions where you will find the following services:

Interactive problem solver

Symantec's online interactive problem solver (known as the Support Genie) helps you solve problems and answer questions about many Symantec products.

Product knowledgebases

Product knowledgebases enable you to search thousands of documents used by Symantec Support Technicians to answer customer questions.

FAQs

Frequently Asked Questions documents, also known as FAQs, list commonly asked questions and clear answers for specific products.

Discussion groups

Discussion groups provide a forum where you can ask questions and receive answers from Symantec online support technicians.

FTP

Point your web browser to <http://service.symantec.com> to search for and download technical notes and software updates. You can also click the LiveUpdate button in programs enabled with this feature to automatically download and install software updates and virus definitions.

Other Symantec support options include the following:

America Online	Type Keyword: SYMANTEC to access the Symantec forum.
CompuServe	Type GO SYMANTEC to access the Symantec forum.
Symantec BBS	Set your modem to 8 data bits, 1 stop bit, no parity and dial (541) 484-6669.
Automated fax retrieval system	<p>To receive general product information, fact sheets and product upgrade order forms directly to your fax machine, please call our Customer Service fax retrieval system at (800) 554-4403 or (541) 984-2490.</p> <p>For technical application notes, please call our Technical Support fax retrieval system at (541) 984-2490 and select option 2.</p>
StandardCare Support	<p>If you can't access the Internet, take advantage of your 90 days of free telephone technical support (from the date of your first call) at no charge to all registered users of Symantec software.</p> <p>Please see the back of this manual for the support telephone number for your product.</p>
PriorityCare and PlatinumCare Support	Expanded telephone support services are available to all registered customers. For complete information, please call our automated fax retrieval service, located in the United States, at (800) 554-4403 or (541) 984-2490, and request document 070, or visit www.symantec.com/techsupp/phone/index.html

Chat Now!

Chat Now! For selected products this service provides customers with the ability to discuss technical issues with a Support Analyst in “realtime” over the Internet, using text, files, and HTML for a fee.

Support for old and discontinued versions

When a new version of this software is released, registered users will receive upgrade information in the mail. Telephone support will be provided for the previous version for six months after the release of the new version. Technical information may still be available through online support.

When Symantec announces that a product will no longer be marketed or sold, telephone support will be discontinued 60 days later. Support will only be available for discontinued products through online services. See the section “Technical support” for online service options.

Customer Service

Symantec’s Customer Service department can assist you with non-technical questions. Call Customer Service to:

- Order an upgrade.
- Subscribe to the Symantec Support Solution of your choice.
- Fulfill your request for product literature or demonstration disks.
- Find out about dealers and consultants in your area.
- Replace missing or defective CDs, disks, manuals, etc.
- Update your product registration with address or name changes.

You can also visit Customer Service online at www.symantec.com/custserv for the latest Customer Service FAQs, to find out the status of your order or return, or to post a query to a Customer Service discussion group.

Worldwide Service and Support

Symantec provides Technical Support and Customer Service worldwide. Services vary by country and include International Partners who represent Symantec in regions without a Symantec office. For general information, please contact the Symantec Service and Support Office for your region.

Service and Support offices

NORTH AMERICA

Symantec Corporation	(800) 441-7234 (USA & Canada)
175 W. Broadway	(541) 334-6054 (all other locations)
Eugene, OR 97401	Fax: (541) 984-8020
Automated Fax Retrieval	(800) 554-4403
	(541) 984-2490

BRAZIL

Symantec Brazil	+55 (11) 5561 0284
Av. Juruce, 302 - cj 11	Fax: +55 (11) 5530 8869
São Paulo - SP	
04080 011	
Brazil	

EUROPE

Symantec Ltd.	+31 (71) 408 3111
Schipholweg 103	Fax: +31 (71) 408 3150
2316 XC Leiden	
The Netherlands	
Automated Fax Retrieval	+31 (71) 408 3782

ASIA/PACIFIC RIM

Symantec Australia Pty. Ltd.	+61 (2) 9850 1000
408 Victoria Road	Fax: +61 (2) 9850 1001
Gladesville, NSW 2111	
Australia	
Automated Fax Retrieval	+61 (2) 9817 4550

Most International Partners provide Customer Service and Technical Support for Symantec products in your local language. For more information on other Symantec and International Partner locations, please call our Technical Support automated fax retrieval service, in the United States at +1 (541) 984-2490, choose Option 2, and request document 1400.

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

Norton AntiVirus™ for Lotus Notes®

CD Replacement Form

CD REPLACEMENT: After your 60-Day Limited Warranty, if your CD-ROM becomes unusable, fill out and return 1) this form, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer in order to receive CD replacements.

FOR CD REPLACEMENT

Please send me: ☐ CD-ROM Replacement

Name

Company Name

Street Address (No P.O. Boxes, Please)

City State Zip/Postal Code

Country* Daytime Phone

Software Purchase Date

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributor.

Briefly describe the problem:

CD Replacement Price	\$ 10.00
Sales Tax (See Table)	
Shipping & Handling	\$ 4.95
TOTAL DUE	<input type="text"/>

SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%). Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT ** (Check One):

☐ Check (Payable to Symantec) Amount Enclosed \$ ☐ Visa ☐ Mastercard ☐ American Express

Credit Card Number Expires

Name on Card (please print) Signature

****U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.**

MAIL YOUR DISK REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
175 West Broadway
Eugene, OR 97401-3003

Please allow 2-3 weeks for delivery within the U.S.

Symantec and Norton AntiVirus are trademarks of Symantec Corporation.
Other brands and products are trademarks of their respective holder/s.
© 1998 Symantec Corporation. All rights reserved. Printed in the U.S.A.

I N D E X

A

- accessing
 - NAV Log, 25
 - Norton AntiVirus, 16
- Add Attachments option, 29
- attachments, 26
 - managing infections, 28
 - viruses and, 10
- automatic updates, 32
- Auto-Protect
 - configuring, 18–20
 - form, 19
 - option, 18

B

- Backup Documents log view, 26
- Basics section, 18
- BBS, Symantec, 31
- Bloodhound technology, 10, 23
- Bulletin Board System. *See* BBS

C

- commands, 17
- computer virus. *See* virus
- configuring
 - LiveUpdate, 31
 - Norton AntiVirus, 9
 - scans, 18–24
- console commands, 17
- current protection, maintaining, 31–33

D

- definitions file, virus, 10
- Delete Attachments option, 29
- disk space requirement, 11
- document backups, 22, 26

- downloading

- Intelligent Updater, 33
 - program patches, 31

E

- email, infected, 28
- Excel. *See* Microsoft Excel

F

- forms
 - Auto-Protect scan, 19
 - Global Options, 21
 - Scan Now, 21
 - Scheduled Scan, 20

G

- Global Options
 - form, 21
 - processing, 23
 - scan, 22
 - virus detection notifications, 24

H

- HELP command, 17
- help, online, 16
- heuristic technology, 10

I

- infected
 - attachments, managing, 28
 - email, 28
- initiating scans, 18
- installation requirements, 11
- installing Norton AntiVirus, 11–12

Intelligent Updater
 description, 33
 downloading, 33
Internet, 31

J

JOBS command, 17

L

LiveUpdate
 automatic, 32
 configuring, 31
 description, 10, 31
 immediate update, 32
 replicating virus definitions database, 15
 scheduling, 32
 updating virus protection
 with, 32
 without, 33
log views, 26
logging options, 22, 23
Lotus Notes
 partitions, 12
 server console window, 17
 virus threat, 10

M

macro virus, 10
maintaining protection, 31–33
managing
 infected attachments, 28
 Quarantine, 26–30
 Quarantine items, 27
memory requirements, 11
Microsoft Excel, 10
Microsoft Word, 10

N

NAV Log
 accessing, 25
 replicating, 13
 using, 25–30
NAV Settings, replicating, 13
Norton AntiVirus
 accessing, 16
 Bloodhound technology, 10, 23
 commands, 17
 configuration, 9
 configuring scanning, 18–24
 console commands, 17
 description, 9–10
 functions, 10
 getting started, 16–17
 help, 16
 installing, 11–12
 LiveUpdate, 10
 maintaining protection, 31–33
 system requirements, 11
Notes. *See* Lotus Notes
Notifications section, 18

O

OLE objects, viruses and, 10
online help, 16
operating system requirements, 11
options
 logging, 23
 processing, 23
 scanning, 18
 virus detection notifications, 24

P

patches, program, 31
Pentium processor, 11
processing options, 23
processor requirement, 11

- program
 - patches, downloading, 31
 - virus, 10
- protection
 - maintaining, 31–33
 - updating
 - with LiveUpdate, 32
 - without LiveUpdate, 33

Q

- Quarantine
 - infected attachments, 28–30
 - items, 27
 - managing, 26–30
- Quarantine Item document, 30
- Quarantined Documents log view, 26
- QUIT command, 17

R

- README.TXT, 12
- replicating
 - NAV log, 13
 - NAV settings, 13
 - virus definitions database, 15
- requirements, system, 11

S

- Save Attachments option, 29
- SCAN command, 17
- Scan Now
 - configuring, 18
 - form, 21
 - option, 18
- Scan Reports log view, 26
- scanning
 - Auto-Protect form, 19
 - configuring, 18–30
 - initiating, 18
 - notifications, 18

- scanning (*continued*)
 - options, 18, 21–24
 - Scan Now form, 21
 - Scheduled Scan form, 20
- Scheduled Scan
 - configuring, 18, 20
 - form, 20
 - multiple servers, 20
 - option, 18
- scheduling LiveUpdate, 32
- scheduling scans, 20
- Server Messages log view, 26
- signature, virus, 10
- starting Norton AntiVirus, 16–17
- STOP command, 17
- Symantec
 - BBS, 31
 - website, 10, 31
- system requirements, 11

U

- updating
 - virus definitions files, 33
 - virus protection
 - with LiveUpdate, 32
 - without LiveUpdate, 33
- using NAV Log, 25–30

V

- virus
 - as attachment, 10
 - as OLE object, 10
 - definition, 10
 - definitions file, 10
 - Lotus Notes, 10
 - macro virus, 10
 - program virus, 10
 - signature, 10
 - updating definitions files, 33
 - updating protection
 - with LiveUpdate, 32
 - without LiveUpdate, 33

virus definitions database, replicating, 15
virus detection notifications, 24
Virus Incidents log view, 26

W

website, Symantec, 10, 31
Windows NT Server requirements, 11
Word. *See* Microsoft Word